July 13, 2006

# HOW TO MAKE WARRANTLESS ELECTRONIC SURVEILLANCE ACCOUNTABLE WITHOUT ENDANGERING NATIONAL SECURITY*

**Richard A. Posner**†

The best, and probably the only, way to end the debate over the propriety of the National Security Agency's conducting electronic surveillance outside the framework of the Foreign Intelligence Surveillance Act is for Congress to amend the Act to create a legal regime that will enable such surveillance to be conducted without infringing civil liberties or invading privacy—but also without compromising national security.

FISA, enacted in 1978—long before the danger of global terrorism was recognized and electronic surveillance was transformed by the digital revolution—is dangerously obsolete. It retains value as a framework for monitoring the communications of known terrorists, but it is hopeless as a framework for detecting terrorists. It requires that surveillance be conducted pursuant to warrants based on probable cause to believe that the target of surveillance *is* a terrorist, when the desperate need is to find out *who* is a terrorist. In the words of General Michael Hayden, director of NSA on 9/11 and now director of the CIA, the NSA program is designed to "detect and prevent," whereas "FISA was built for long-term coverage against known agents of an enemy power." Yet in combatting terrorism "the

---

* Testimony prepared for a hearing on "Modernization of the Foreign Intelligence Surveillance" before the House Permanent Select Committee on Intelligence, to be held on July 19, 2006.

† The author is a judge of the U.S. Court of Appeals for the Seventh Circuit and a senior lecturer at the University of Chicago Law School. He has written extensively on national-security intelligence, including two recent books: *Preventing Surprise Attacks: Intelligence Reform in the Wake of 9/11* (2005), and *Uncertain Shield: The U.S. Intelligence System in the Throes of Reform* (2006).

problem of defeating the enemy consists very largely of finding him."‡

Critics of NSA's program point out that surveillance not cabined by a probable-cause requirement produces many false positives (intercepts that prove upon investigation to have no intelligence value). That is not a sound criticism. National security intelligence is a search for a needle in a haystack. The intelligence services must cast a wide net with a fine mesh to catch the clues that may enable the next terrorist attack on the United States to be prevented. The initial trolling for clues is done by computer search programs, which do not invade privacy because search programs are not sentient beings. The programs pick out a tiny percentage of communications to be read by (human) intelligence officers, and a subset of these communications will turn out to have intelligence value and spur an investigation.§ Some of these may be communications to which a U.S. citizen or permanent resident is a party.

The NSA is also believed to have obtained millions of phone records from telephone companies to enable the agency to engage in "traffic analysis." That means analyzing the phone traffic (the outside of the envelope, as it were) rather than the contents of the phone conversations (the inside of the envelope). Suppose the NSA has the phone number of a known or suspected terrorist. It can use its database of phone numbers to determine the most frequent numbers called to or from that number and then determine the most frequent numbers called to or from *those* numbers and in this way trace a possible terrorist network—all without listening to any conversation. That comes later.

Such programs are vital, given the terrorist menace, which is real—and, as recent terrorist activities in places as far apart

---

‡ Frank Kitson, quoted in Bradley W. C. Bamford, "The Role and Effectiveness of Intelligence in Northern Ireland," 20 *Intelligence and National Security* 581, 586 (2005).

§ For a lucid description of how such surveillance works, see K. A. Taipale, "Whispering Wires and Warrantless Wiretaps: Data Mining and Foreign Intelligence Surveillance" (forthcoming, *N.Y.U. Review of Law and Security*, spring 2006).

as Canada, Israel, and India suggest, are growing. This city, the capital of the United States, could be destroyed by an atomic bomb the size of a melon, which if coated with lead would be undetectable. The city could be rendered uninhabitable, perhaps for decades, merely by the explosion of a conventional bomb that had been coated with radioactive material. Smallpox virus bioengineered to make the virus even more toxic and the vaccine ineffectual, then aerosolized and sprayed in a major airport, could kill millions of people. Our terrorist enemies have the will to do such things and abundant opportunities, because our borders are porous both to enemies and to containers. They will soon have the means as well. Access to weapons of mass destruction is becoming ever easier, especially access to biological weaponry, which is simple and cheap to make and easy to conceal and disseminate.

Most likely the next terrorist attack on the United States, like the 9/11 attacks, will be mounted from inside the country but be orchestrated by leaders safely ensconced somewhere abroad. So suppose the NSA learns the phone number of a suspected terrorist in a foreign country. If the agency wants just to listen in to his calls to other people abroad, FISA doesn't require a warrant. But it does if either (1) one party to the call is in the United States and the interception takes place here or (2) the party on the U.S. side of the conversation is a "U.S person"—primarily either a citizen or a permanent resident. If both parties are in the United States, no warrant *can* be issued; interception is prohibited. But as a practical matter the government cannot get a warrant in the "U.S. person" situation either, in the case that I have posited, because the statute requires grounds for believing that such a person is a foreign spy or a terrorist. Even if a person is here just on a student or tourist visa, or on no visa, the government can get a warrant only if it has probable cause to believe him an agent of a foreign power or a terrorist group. In either case, the government can't get a warrant just to find out whether someone is a terrorist; it has to already have a reason to believe that he is one.

It may be thanks to programs such as the NSA's non-FISA surveillance, as well as to other counteterrorist operations,

that we have been spared a repetition of 9/11. We must not let our guard down, basking in the false assurance created by the lapse of time since the last attack. The legality of the NSA program has been called into question, and fears have been expressed about its impact on civil liberties and on privacy. Fortunately, Congress can allay these concerns without gutting the program. But not by amending FISA to relax the standard for obtaining a warrant. Instead of requiring probable cause to believe the target a terrorist, FISA could, no doubt, be amended to require merely reasonable suspicion. But even that would be too restrictive. It is not enough to be able to monitor suspects; they must be found. Moreover, the lower the standard for getting a warrant, the more porous the filter that a requirement of a warrant creates. If all that the government is required to state in its application for a warrant is that it thinks an interception might yield intelligence information, judges will have no basis for refusing to grant the application. The requirement of a warrant will be a figleaf.

The preoccupation of civil libertarians with warrants is anachronistic. The government's easy access to the vast databases compiled by private and public entities for purposes unrelated to national security has enabled it to circumvent the privacy interests that civil libertarians look to warrant requirements to protect.** Fortunately, other modes of protecting civil liberties and privacy are available. Concretely, I suggest that Congress amend FISA to authorize warrantless electronic surveillance to obtain national-security intelligence but at the same time subject that surveillance to tight oversight and specific legal controls, as follows:

1. *Oversight*: The amendment would—

a. Create a steering committee for national security electronic surveillance composed of the Attorney General, the Director of National Intelligence, the Secretary of Homeland Security (chairman), and a senior or retired federal judge or Justice appointed by the Chief Justice of the United States. The

** See, for example, Arshad Mohammed and Sara Kehaulani Goo, "Government Increasingly Turning to Data Mining: Peek into Private Lives May Help in Hunt for Terrorists," *Washington Post*, June 15, 2006, p. D3.

committee would monitor all such surveillance to assure compliance with the Constitution and laws.

b. Require the NSA to submit to the FISA court, every six months, a list of the names and other identifying information of all persons whose communications had been intercepted without a warrant in the preceding six months, with a brief statement of why these individuals had been targeted. If the court concluded that an interception had been inappropriate, it would so report to the steering committee and the congressional intelligence oversight committees. Alternatively, the list could be required to be submitted directly to the oversight committees. In addition, judicial officers employed by the FISA court could be stationed in the NSA to monitor its data-mining activities for compliance with law.

2. *Specific controls*: The amendment would—

a. Authorize "national security electronic surveillance" outside FISA's existing framework, provided that the President certified that such surveillance was necessary and proper in the national interest. Warrants would continue to be required for all physical searches and for all electronic surveillance for which FISA's existing probable-cause requirement could be satisfied.

b. Define "national security" narrowly, excluding "ecoterrorism," animal-rights terrorism, and other forms of political violence that, though criminal and deplorable, do not endanger the nation.

c. Sunset after five years, or sooner if the declaration of national emergency was rescinded.

d. Forbid *any* use of intercepted information for any purpose other than "national security" as narrowly defined in the amendment (point b above). Thus the information could not be used as evidence or leads in a prosecution for ordinary crime. Violations of this provision would be made felonies punishable by long prison sentences and heavy fines, to allay concern that "wild talk" picked up by electronic surveillance would lead to criminal investigations unrelated to national security. No one wants strangers eavesdropping on his personal conversations. But the principal reason for this aversion is fear of what the

strangers might do with the information to harm one, and that fear can be allayed by forbidding the use of information obtained by surveillance conducted to detect terrorist activity for any purpose other than to protect national security. So if the NSA discovered that an American was not a terrorist but was evading income tax, it could not refer its discovery to the Justice Department or the Internal Revenue Service to enable the person to be prosecuted for tax evasion or sued for back taxes.

e. Require responsible officials to certify to the FISA court annually that there had been no violations of the statute during the preceding year. False certification would be punishable as perjury.

f. Bar lawsuits challenging the legality of the NSA's current warrantless surveillance program. Such lawsuits would distract officials from their important duties, to no purpose given the amendment.

The point to be particularly emphasized is that warrants are neither the best nor the only method of allaying the concerns that comprehensive electronic surveillance for purposes of national-security intelligence engenders. By amending FISA to place such surveillance under high-level supervision, restrict (under pain of heavy criminal penalties) the uses that can be made of information obtained by the surveillance, assure judicial and congressional access to the records of the surveillance, and establish the other controls that I have suggested, Congress can protect civil liberties and privacy without undermining national security.